Amendments to the Claims

1. (Previously Presented) A method of providing a value note comprising:

providing first information representative of a bearer's public key information, or from which a bearer's public key information can be verified;

providing second information representative of a commodity represented by the value note; and

calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of an issuer's public key information.

Claim 2 (cancelled)

3. (Previously Presented) A method according to claim 1, further comprising providing information on when the value note is due to expire.

4. (Previously Presented) A method according to claim 3, wherein the expiry information is included in the calculation of the third information.

5. (Previously Presented) A method according to claim 1, further comprising providing identification information for uniquely identifying the value note.

6. (Original) A method according to claim 5, wherein the identification information comprises a serial identification string.

7. (Previously Presented) A method according to claim 5, wherein the identification information is included in the calculation of the third information.

8. (Previously Presented) A method according to claim 1, further comprising providing valid-from information representing from when the value note is available for redemption.

9. (Previously Presented) A method according to claim 8, wherein the valid-from information is included in the calculation of the third information.

10. (Previously Presented) A method according to claim 1, further comprising communicating the value note electronically.

11. (Original) A method according to claim 10, wherein the value note is sent through an electronic public communication system.

12. (Previously Presented) A method according to claim 1, wherein the issuer's signature is an RSA type signature.

13. (Previously Presented) A method of handling a value note, comprising:

receiving a value note comprising first information either representative of a bearer's public key or from which bearer's public key can be verified, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and an issuer's public key information;

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the redemption instruction information and is verifiable from said first information.

14. (Original) A method according to claim 13, wherein the bearer's signature is an RSA type signature.

15. (Previously Presented) A method according to claim 13, wherein the value note is provided by:

providing first information representative of a bearer's public key information, or from which the bearer's public key information can be verified;

providing second information representative of a commodity represented by the value note; and

calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of the issuer's public key information.

16. (Previously Presented) A method according to claim 13, wherein the step of providing the bearer's signature comprises calculating the signature based on information including the redemption instruction information and a secret key related to the first information.

17. (Original) A method according to claim 16, wherein said information on which the bearer's signature is calculated includes information from the value note.

18. (Previously Presented) A method according to claim 13, wherein the redemption instruction information includes a reference to transfer at least a portion of the commodity to a first new value note.

19. (Previously Presented) A method according to claim 18, wherein the redemption instruction information includes replacement first information for the first new value note.

20. (Previously Presented) A method according to claim 18, wherein the first new value note has a different bearer's public key from the value note being redeemed.

21. (Previously Presented) A method according to claim 18, wherein the redemption instruction information includes a reference to transfer a remainder of the commodity to a second new value note.

22. (Original) A method according to claim 21, wherein the second new value note has a different bearer's public key from the value note being redeemed.

23. (Previously Presented) A method according to claim 18, wherein the redemption instruction information includes a reference to transfer the commodity represented by the first new value note to a replacement new value note if the first new value note is not redeemed within a predetermined period.

24. (Original) A method according to claim 23, wherein the replacement new value note has a different bearer's public key from the first new value note.

25. (Previously Presented) A method according to claim 13, wherein the redemption instruction information includes an identification reference for each value note referred to in the redemption instruction information, and wherein the method comprises communicating the redemption instruction information to a value note handling authority.

26. (Previously Presented) A method according to claim 13, further comprising communicating the value note, the redemption instruction information and the bearer's signature information to a value note handling authority.

27. (Previously Presented) A method according to claim 25, wherein the communication is effected over an electronic public communication system.

28. (Previously Presented) A method of handling redemption instruction information and bearer signature information associated with a value note, the method comprising performing at least one verification prior to redeeming the value note in accordance with the redemption instruction information, the verification comprising:

verifying that the bearer signature information matches information including at least the redemption instruction information using the bearer's public key information presented in the value note or in the redemption instruction information.

29. (Original) A method according to claim 28, wherein the redemption instruction information is associated with a plurality of value notes.

30. (Previously Presented) A method according to claim 28, further comprising:

receiving a value note comprising first information representative of a bearer's public key or from which bearer's public key can be verified, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and the issuer's public key information;

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the redemption instruction information and is verifiable from said first information.

31. (Previously Presented) A method according to claim 28, wherein the redemption instruction information and the bearer signature information are received without a value note, and the method comprises retrieving value note information for one or more value notes identified in the redemption instruction information.

32. (Previously Presented) A method according to claim 28, further comprising verifying that an issuer signature included in the value note matches information including the bearer's public key information and a commodity represented by the value note, using an issuer's public key information.

33. (Previously Presented) A method according to claim 28, further comprising verifying that the value note has not previously been presented for redemption.

34. (Previously Presented) A method according to claim 28, further comprising verifying that the value note has not previously been redeemed validly.

35. (Previously Presented) A method according to claim 33, wherein at least one of the value note and the redemption instruction information includes identification information for uniquely identifying the value note, and the verification comprises ascertaining whether a value note bearing the same identification information has previously been accepted.

36. (Previously Presented) A method according to claim 28, further comprising verifying whether a counter signature matches a counter signatory's public key information in the value note.

37. (Previously Presented) A method according to claim 28, further comprising verifying whether an endorsement signature in the value note matches information including a predefined message using a message endorsing signatory's public key information.

38. (Previously Presented) A method according to claim 28, wherein the value note includes expiry information representing at least one of a time and a date of expiry, and the method further comprises testing the value note on the basis of the expiry information.

39. (Previously Presented) A method according to claim 28, wherein the value note includes valid-from information representing at least one of a time and a date from which the value note may validly be redeemed, and the method further comprises testing the value note on the basis of the valid-from information.

40. (Previously Presented) A method according to claim 28, further comprising redeeming the value note in accordance with the redemption instruction information, wherein the step of redeeming the value note comprises issuing a first new value note representing at least a portion of the commodity of the value note being redeemed.

41. (Original) A method according to claim 40, wherein first new value note includes different public key information from the value note being redeemed.

42. (Previously Presented) A method according to claim 40, wherein the step of redeeming the value note comprises issuing a second new value note representing a remainder of the commodity of the value note being redeemed.

43. (Original) A method according to claim 42, wherein the second new value note includes a different bearer public key from the value note being redeemed.

44. (Previously Presented) A method according to claim 40, wherein the step of redeeming the value note comprises issuing a replacement new value note if said first new value note is not redeemed within a predetermined period.

45. (Original) A method according to claim 44, wherein the replacement value note includes a different bearer's public key from the value note being redeemed.

46. (Previously Presented) A method according to claim 40, wherein at least one new value note is issued which includes information indicative of at least one of a time and a date from which the new value note can be redeemed, and wherein the at least one of a time and a date is later than either a time or a date of issuance.

47. (Previously Presented) A method according to claim 28, further comprising communicating each value note electronically to a remote party corresponding to the source of the value note being redeemed.

48. (Original) A method according to claim 47, wherein the communication is effected over a public communication system.

Claims 49 and 50 (cancelled).

51. (Previously Presented) A method according to claim 18, wherein the method comprises generating a first character string message, generating a second character string message from said first message in the redemption instruction information for inclusion in the first new value note.

52. (Currently Amended) A method <u>of handling a value note,</u> ~~according to claim 51, further~~ comprising the steps of:

<u>receiving a value note comprising first information either representative of a bearer's public key or from which bearer's public key can be verified, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and an issuer's public key information;</u>

<u>providing redemption instruction information for the value note that includes a reference to transfer at least a portion of the commodity to a first new value note;</u>

providing a bearer's signature which is dependent on the redemption instruction information and is verifiable from said first information;

generating a first character string message, generating a second character string message from said first message in the redemption instruction information for inclusion in the first new value note.

communicating the value note, the redemption instruction information, and the bearer's signature information to a value note handling authority;

applying a blinding function to the second character string message to generate a blinded second character string message;

issuing the first new value note including the blinded second character string message, in accordance with the redemption instruction information;

communicating the first new value note to a respondent; and

providing endorsement signature information from the respondent dependent on the first and second character string message and related to the blinding function such that the endorsement signature information is verifiable against both the first character string message and the second character string message; and

communicating the first value note with the respondent's endorsement signature information to a value note handling authority.

53. (Previously Presented) A method according to claim 52, further comprising the step of unblinding the blinded second character string message by the respondent to yield the first character string message prior to providing the respondent's endorsement signature information.

Claims 54-60 (Cancelled).

61. (Previously Presented) A value note comprising:

first information representative of a bearer's public key information or from which the bearer's public key information can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and the issuer's public key information.

62. (Previously Presented) A record carrier on which is recorded value note information including:

first information representative of a bearer's public key information, or from which the bearer's public key information can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and the issuer's public key information.

63. (Previously Presented) A transmission signal representing a value note and comprising:

first information representative of a bearer's public key information, or from which the bearer's public key information can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and the issuer's public key information.

Claim 64 (cancelled)

65. (Currently Amended) A method of providing redemption instruction information for one or more value notes each being as defined in claim 63, the method comprising:

providing a list of identification information for identifying each existing value note to be used in ~~[[the]]~~ a transaction;

providing a list of redemption requests, each request including information representing a result of the transaction, and a commodity value associated with that result;

providing a bearer's signature information representing a bearer's signature which is verifiable at least one of the redemption instruction information and information in said value notes, and the bearer's public key information.

66. (Previously Presented) A method according to claim 65, wherein at least one redemption request includes a request to issue a new value note.

67. (Previously Presented) A method according to claim 65, further comprising providing information representing the bearer's public key information.

68. (Previously Presented) A method according to claim 65, further comprising providing information representing the total value of the existing value notes, which total value is to divided or allocated in accordance with the list of redemption requests.

69. (Previously Presented) A method according to claim 65, further comprising communicating the redemption instruction information, with or without the individual value notes referred to in the redemption instruction information, to a money handling authority.

Claims 70-73 (Cancelled).

74. (Previously Presented) Apparatus for carrying out a method as defined in claim 1, comprising at least one bank terminal, at least one user terminal, and a network interconnecting the at least one bank terminal and the at least one user terminal over which the value note can be communicated.